IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JENNIFER CLEMENS, individually and on behalf of all others similarly situated, Plaintiff, v. EXECUPHARM, INC., Defendant.	Case No.: 2:20-cv-03383-GJP **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Jennifer Clemens ("Plaintiff"), by and through her undersigned counsel, brings this First Amended Class Action Complaint against Defendant ExecuPharm, Inc. (hereafter "ExecuPharm" or "Defendant"), individually and on behalf of all others similarly situated, and alleges as follows, based upon personal knowledge as to herself, and upon information and belief as to all other matters.

INTRODUCTION

1. ExecuPharm is a Pennsylvania-based subsidiary of global biopharmaceutical giant Parexel that provides clinical research support services for the pharmaceutical industry. On March 13, 2020, ExecuPharm suffered a serious data breach whereby third-party hackers gained access to troves of sensitive information maintained on ExecuPharm's servers and demanded a ransom in exchange for not releasing the information (the "Data Breach").

2. The stolen information included, among other sensitive information, full names, home addresses, social security numbers, taxpayer IDs, credit card numbers, banking information (including copies of personal checks for direct deposit), driver's licenses, dates of birth, names of spouses and beneficiary information, including their social security numbers, payroll tax forms

(such as W-2 and W-4 forms), and in some cases, copies of passports (collectively "Personal Information") of ExecuPharm's current and former employees, as well as certain Parexel employees whose information was stored on ExecuPharm's servers. After ExecuPharm failed to meet the hackers' demands, this information was posted to a dark web website associated with a well-known ransomware group, along with thousands of emails, financial and accounting records, user documents, and database backups.

3. Those individuals impacted by the Data Breach are now at serious risk. Their most sensitive personal and financial information is in the possession of cybercriminals seeking to profit from it and is freely available on underground websites for anyone to access. Even ExecuPharm acknowledged the immediate danger affected individuals face, advising them to "act diligently and immediately in the face of heightened likelihood of bad actors using your information unlawfully and/or without your consent" and to "take every precautionary measure."

4. Consequently, thousands of individuals have suffered or are at an imminent risk of identity theft and fraud, and will face a lifetime of expensive and time-intensive efforts to mitigate the actual and potential impact of the Data Breach, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their financial accounts and credit reports for unauthorized activity.

5. ExecuPharm is responsible for the breach by failing to implement and maintain reasonable safeguards to protect its employees' information and failing to comply with industry-standard data security practices, contrary to the promises made in their employment agreements. Plaintiff brings this action on behalf of herself and those similarly situated to seek redress for the lifetime of harm they will now face, including reimbursement of losses associated with identity

theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extended credit monitoring services and identity theft insurance, and injunctive relief requiring ExecuPharm to implement and maintain reasonable data security practices going forward.

PARTIES

6. Plaintiff Jennifer Clemens is a former employee of ExecuPharm and current resident and citizen of Sanford, Florida.

7. Defendant ExecuPharm is a wholly owned subsidiary of Parexel International Corp., with its principal place of business located at 610 Freedom Business Center Drive, Suite 200, King of Prussia, Pennsylvania 19406.

8. Defendant is represented by counsel and may be served with this First Amended Complaint through its counsel of record.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which at least one member of the class is a citizen of a state different from Defendant, the amount in controversy exceeds $5 million exclusive of interest and costs, and the proposed class contains more than 100 members.

10. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(2) and (c)(2) because a substantial part of the events or omissions giving risk to the claim occurred here and Defendant is subject to this Court's personal jurisdiction. Among other things, ExecuPharm is headquartered in this District, Defendant conducts substantial business operations in this District, and purposely availed itself to the benefits of the Court's jurisdiction.

FACTUAL ALLEGATIONS

The Data Breach

11. Founded in 1995, ExecuPharm markets itself as a leading global functional service provider for the biopharmaceutical industry, including providing support services for clinical trials. In October 2016, ExecuPharm was acquired by Parexel, a global provider of biopharmaceutical services with annual revenues exceeding $2.4 billion.

12. On or before March 13, 2020, certain ExecuPharm employees received "phishing" emails from unknown hackers seeking sensitive information. These e-mails may have contained a malicious link or attachment or were crafted to appear as if they came from a known source seeking login credentials or other internal information that could be used to gain access to ExecuPharm's networks.

13. On or about March 13, 2020, the hackers used the information obtained from successful phishing attempts to access ExecuPharm's servers and install malicious software known as "malware." The malware was used to encrypt the data stored on ExecuPharm's servers, rendering it indecipherable, and included a ransom demand in exchange for the decryption tools. The hacking group also exfiltrated the data from ExecuPharm's network, threatening to release it if the ransom was not timely paid.

14. ExecuPharm later attributed the breach to the CLOP ransomware group, whose signature is encrypting a company's internal data and renaming it with a ".Clop" extension on the end (for example, "sample.jpg" is renamed to "sample.jpg.Clop").[1] According to PCrisk.com,

[1] T. Meskauskas, *Clop ransomware removal instructions*, PCRISK (March 25, 2020), https://www.pcrisk.com/removal-guides/14451-clop-ransomware (last visited Sept. 5, 2023).

following successful encryption, CLOP will generate a text file placed in every folder called "ClopReadMe.txt" which contains a ransom demand message.[2]

15. Within approximately six weeks of the unauthorized access, the stolen ExecuPharm information was posted on underground websites known as the "dark web." The dark web is a portion of the Internet that is intentionally hidden from search engines and requires the use of an anonymizing browser to be accessed. It is most widely used as an underground black market where individuals sell illegal products like drugs, weapons, counterfeit money, and sensitive stolen data that can be used to commit identity theft or fraud.

16. In the weeks leading up to this massive data leak, ExecuPharm notified affected individuals their information was accessed, but withheld critical information regarding the nature of the Data Breach and ransom demand. For example, in its initial letter to ExecuPharm's former employees dated March 18, 2020 (although not received by many until a later date), ExecuPharm stated as follows:

Dear ExecuPharm Alumni:

We are reaching out to inform you of a recent security incident wherein malicious, phishing-type emails were sent out to several of our current and former employees over this past weekend or early this week. We now know that the people behind these emails have accessed and shared select corporate and personal information relating to ExecuPharm personnel as well as former ExecuPharm employees.

Safeguarding the security of our data is one of our highest priorities, and we do not take events like this lightly. While our investigation is still ongoing, we wanted to update you on some key developments:

- **Upon learning of the potential incident, ExecuPharm immediately notified federal and local law enforcement authorities, retained leading data security forensics firms to investigate the nature and scope of the potential incident, and contacted our insurer to make certain we are following the proper cybercrime response and fortifying our systems**.
    - This includes installing supplemental forensic tools on all systems and isolating impacted systems until we confirm that they are secure.

[2] *Id*.

- We are also implementing countermeasures to block further ransomware emails

- **If you are receiving this email, we believe you may be among the group of former employees impacted by this incident. Please know we take our responsibility to protect your information very seriously and we recognize the trust you place in us**.
  - ExecuPharm will be offering complimentary credit monitoring/identity theft protection services to those individuals whose information may have been inappropriately accessed, and in the coming days we will work quickly to provide you with additional resources to help protect your information.
  - In the meantime, we encourage you to place a fraud alert on your credit file (creditors will contact you before they open new accounts or change your existing accounts), check your credit report (and freeze your credit if you have concerns), change passwords to any personal accounts that you may have been accessed on the ExecuPharm server, and actively monitor financial statements for suspicious activity.
  - To place a fraud alert on your credit file, you may contact one of the credit bureau's below. When one of the bureaus confirms your fraud alert, the others are notified to place fraud alerts as well. This alert is good for one year, and renewable upon expiration of the year term. You can also request that all three bureaus send credit reports to you for review, free of charge.
    a. Equifax: equifax.com(link is external) or 1-800-685-1111
    b. Experian: experian.com(link is external) or 1-888-397-3742
    c. TransUnion: transunion.com(link is external) or 1-888-909-8872

17. This letter raised more questions than it answered. First, the letter failed to disclose what information was compromised in the breach, essential information given that different precautions may be necessary depending on what type of information is involved. Second, the letter omitted altogether that the group behind the hack was a known ransomware group that threatened to release the information if certain conditions were not met. Had affected individuals been informed of this fact, they could have taken immediate measures to protect themselves knowing that the release of their information was potentially imminent. Finally, the letter promised "complimentary credit monitoring/identity theft protection services," but provided no further information on when and what services would be made available or how long such protections would be in effect. Again, this caused affected individuals to delay in taking preventative actions while waiting for additional information from ExecuPharm.

18. Perhaps recognizing these deficiencies, ExecuPharm sent a follow-up e-mail notification on March 20, 2020 to certain individuals disclosing what information was actually impacted: "Unfortunately, we now believe sensitive information has been accessed, including social security number, banking information (copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including social security numbers) and payroll tax forms (such as W-2 and W-4). For some employees, copies of passports also were accessed."

19. This communication again stated that credit monitoring services would be made available and that "[t]o activate these services and provide you with additional information, we have set up a dedicated hotline beginning March 23. Look for more information on this soon — this team will be able to activate monitoring support and walk you through other services. We have elected for the highest level of service available on a country-specific basis."

20. ExecuPharm also advised affected individuals to take a number of actions to protect themselves against the threat of harm:

> **In the interim, we again encourage you to:**
>
> - Place a fraud alert on your credit file (creditors will contact you before they open new accounts or change your existing accounts)
> - Check your credit report (and freeze your credit if you have concerns)
> - Change passwords to any personal and professional accounts that may have been accessed on the ExecuPharm server
> - Speak with your bank representative for specific guidance on any changes that may be needed to your bank account(s).
> - Actively monitor financial statements for suspicious activity
> - File taxes as soon as possible to mitigate any potential fraudulent tax filing activity

21. While not accepting responsibility, ExecuPharm's communication concluded with an acknowledgement of concern: "We completely understand — and share — your frustrations

with this situation. Addressing your concerns and providing you support as you take steps to protect the safety of your information is our priority. We will continue to share pertinent information and communicate candidly with you via email while also providing information on accessing assistance and resources as part of our remediation efforts."

22. Unfortunately, affected individuals who attempted to call ExecuPharm's "dedicated hotline" on March 23 to seek more information or activate their monitoring services were greeted with a disconnect signal. Additionally, despite its commitment to candor, ExecuPharm continued to withhold essential information, including that the group behind the hack was a known ransomware group that threatened imminent release of the stolen information.

23. On March 24, 2020, ExecuPharm sent another follow-up email to address frequently asked questions it received from those impacted:

> We have heard from some of you with the following questions in response to our recent communications about the ExecuPharm security incident and we thought it would be helpful to share our responses for the benefit of all:
>
> **Q: What specific information was compromised for me individually?**
> A: We are working diligently to determine the impact of the security incident at the individual level and we will be communicating that information directly with each impacted individual as soon as possible. In the meantime, we suggest that you take appropriate steps to protect your information.
>
> **Q: What is ExecuPharm doing to prevent this from happening again?**
> A: We take the security and confidentiality of our employee information very seriously. We regret this incident and are currently working with leading cybersecurity firms to further strengthen the security of our computer systems and network infrastructure. We are also implementing additional countermeasures to block further ransomware emails. We will utilize the knowledge we have gained from this experience to further enhance our existing security protocols for the future.

24. On March 25, 2020, affected individuals were notified that the free credit monitoring services offered by ExecuPharm would only be available for one year, a vastly inadequate protection given the lifetime of harm affected individuals now face.

25. Later communications confirm that ExecuPharm knew the stolen information was likely to be released but continued to withhold essential details regarding the identity of the hackers and nature of the ransom demand. For example, on April 13, 2020, ExecuPharm updated its informational website to state: "**We ask that everyone act diligently and immediately in the face of heightened likelihood of bad actors sharing and/or using your information**. To protect yourself, please remain vigilant about any suspicious activity on accounts, and take every precautionary measure, including activating the free identity monitoring and theft protection services we are making available to everyone affected. Our comprehensive investigation of the attack is ongoing. We understand the concerns this incident may be causing, and the company's focus is on resolving the situation as best we can."

26. On April 17, 2020, ExecuPharm stated in an e-mail communication the "critical" importance of activating the credit monitoring services offered "[s]hould the data that was accessed become public":

> As we have shared in previous communications, we believe sensitive information may have been accessed, including social security numbers, banking information, drivers' licenses, dates of birth, home addresses, payroll tax forms (such as W-2 and W-4), and passport numbers. Therefore, ExecuPharm has contracted with global leaders in risk mitigation and response, to provide identity monitoring at no cost to you for one year. Should the data that was accessed become public, the monitoring service will be able to track and alert you if your information is being used. **It is critical you activate your monitoring service to help mitigate your risk of identity theft.**

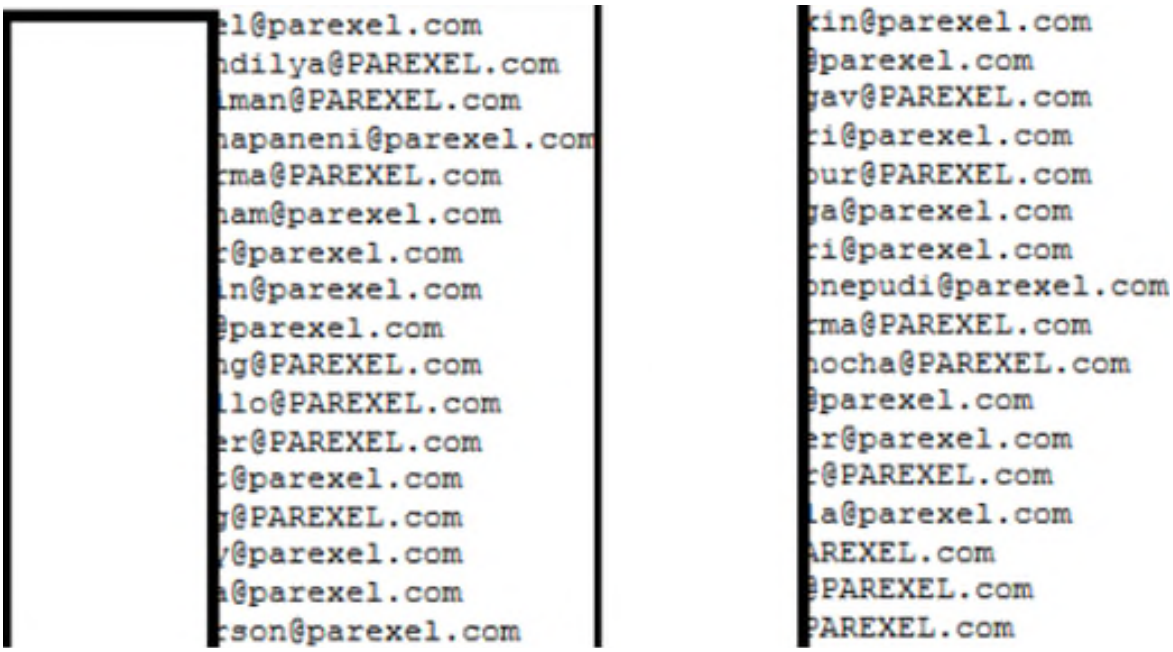
27. In a separate update letter dated April 17, 2020, ExecuPharm confirmed that affected individuals included not only current and former ExecuPharm personnel, but also "select personnel of Parexel, whose information was stored on ExecuPharm's data network."

28. ExecuPharm also confirmed that the stolen information included "social security numbers, taxpayer ID/EIN, driver's license numbers, passport numbers, bank account numbers, credit card numbers, national insurance numbers, national ID numbers, IBAN/SWIFT numbers,

and beneficiary information (including social security numbers)." The company warned that "[u]nauthorized access to such information may potentially lead to the misuse of your personal data to impersonate you and/or to commit, or allow third parties to commit, fraudulent acts such as securing credit in your name."

29. On April 26, 2020, the inevitable was confirmed when an Israel-based intelligence firm tweeted screenshots of a dark web website hosting gigabytes of the stolen ExecuPharm information available for download, which included a sample of Parexel employee information exposed in the breach.[3] The download links contained nearly 123,000 files and 162 gigabytes of data, including nearly 19,000 files of correspondence involving ExecuPharm and Parexel; more than 80,600 e-mail correspondences; financial, accounting, user documents of ExecuPharm's employees and managers; and a complete backup file of ExecuPharm's document management system. The website noted that the next archive of information would be published on April 27, 2020.

[3] Twitter.com/X, https://twitter.com/UnderTheBreach/status/1254382668835434496, @UnderTheBreach, (Apr. 26, 2020) (account no longer active).



>_ CL0P^_- LEAKS

Home IHI-CSI.DE MVTEC.COM NFT.CO.UK POLYVLIES.DE INRIX.COM **EXECUPHARM.COM**

Headquarters:
610 Freedom Business Center Dr., Ste. 200, King of Prussia, Pennsylvania, 19406, United States
Phone:
(610) 272-8771
Website:
www.execupharm.com
Employees:
5,000
Revenue:
$314 Million

FILES:
18895 mails of execupharm and parexel employers DOWNLOAD
Email correspondence 80604 mails 16.4 GB DOWNLOAD

Financial, accounting, user documents of employees and managers.
SQL backups of document management system. Total 11 archives.
Total file count: 122980 Total size: 162GB
ARCHIVE1 DOWNLOAD
Next archive will be published 27/04

Page views: 337

30. That same day, ExecuPharm sent an e-mail communication to affected individuals disclosing that the stolen information was made available on the dark web and acknowledging the "heightened likelihood of bad actors using your information unlawfully and/or without your consent":

> **Dear ExecuPharm Alumni:**
> We are writing to share an important update regarding the data security incident at ExecuPharm. As our investigation has progressed, we have become aware that the **information accessed by the cyberattackers has been shared on the dark web.**
> In light of this, **we strongly encourage those who have not done so to activate the free identity monitoring and theft protection services provided to you without delay.**
> **We ask that everyone act diligently and immediately in the face of heightened likelihood of bad actors using your information unlawfully and/or without your consent.** To protect yourself, please remain vigilant about any suspicious activity on accounts, and take every precautionary measure. If you have any questions or concerns, please call our dedicated incident hotline:
>
> ***
>
> We take this incident extremely seriously and have taken significant affirmative steps to ensure ExecuPharm data is secure. Our comprehensive investigation is ongoing and we will continue to keep you apprised of key developments.

31. In an article published on April 27, 2020, ExecuPharm's vice president of business operations, David Granese, confirmed that CLOP was behind the hack. Granese told TechCrunch in a statement: "ExecuPharm immediately launched an investigation, alerted federal and local law enforcement authorities, retained leading cybersecurity firms to investigate the nature and scope of the incident, and notified all potentially impacted parties."[4]

The Data Breach was Preventable

32. Following the Data Breach, ExecuPharm repeatedly stated that it was "fortifying" its systems and taking "significant affirmative steps to ensure ExecuPharm data is secure." For example, it its April 17, 2020 update letter, ExecuPharm represented that it "implemented

[4] Z. Whittaker, *Hackers publish ExecuPharm internal data after ransomware attack*, TECHCRUNCH (April 27, 2020), https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/ (last visited Sept. 5, 2023).

additional countermeasures to block further ransomware emails from entering the ExecuPharm environment" and "upgraded its security measures to prevent future attacks, including forced password resets, multi-factor authentication for remote access, and endpoint protection, detection, and response tools."

33. But these are industry-standard measures that should have been implemented long before the Data Breach occurred, especially given that pharmaceutical and healthcare industries are frequently the most targeted sectors for phishing scams and cyberattacks.

34. For years "phishing" scams have been the most popular and effective method of gaining authorized access to a company's internal networks. In Verizon's 2019 Data Breach Investigations Report (DBIR), phishing scams were the top threat action in data breaches, with 32% of confirmed breaches having resulted from phishing scams. In addition, 28% of breaches involved malware infections, and 29% involved the use of stolen credentials, both of which are frequently accomplished through phishing attacks.

35. There are two primary defenses to "phishing" scams: employee education and technical security barriers. Employee education is the process of making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common example of a phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. Oftentimes the request comes from a suspicious or unfamiliar e-mail address and may include incorrect spelling or an unusual tone. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

Employee education provides the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of sensitive internal information.

36. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC).

37. Additionally, because the goal of many phishing attempts is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access—even if a phishing attempt is successful. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

38. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes

appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

39. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[5] In an example given by security software provider Digital Guardian, "an employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide."[6] This is precisely why approximately 67% of targeted malware and phishing attacks are directed at individual contributors and lower-level management personnel.[7]

40. Despite housing highly-sensitive data, ExecuPharm did not adhere to these best practices and its implementation of some or all of these measures only after the fact is inexcusable given Defendant's knowledge that it was a prime target for cyberattacks. Chris DeRamus, Chief Technology Officer at cybersecurity firm DivvyCloud Corp., noted that healthcare and pharmaceutical organizations are one of the top targets for cyberattacks, since they house massive

[5] N. Lord, *What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance* (Sept. 12, 2018), https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited Sept. 5, 2023).

[6] *Id*.

[7] J. Davis, *Pharmaceutical Companies Most Targeted Industry by Cybercriminals*, HEALTHITSECURITY (Nov. 30, 2018), https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited Sept. 5, 2023).

troves of personally identifiable information on their patients and customers. "There are no known decryption tools for CLOP ransomware, making this incident affecting ExecuPharm particularly concerning and further demonstrates the need for organizations to implement a more proactive approach to security and compliance practices."[8]

41. Joseph Carson, Chief Security Scientist at security company Thycotic, stated that: "Unfortunately for ExecuPharm, the attackers have started releasing personal data on employees which includes some very sensitive data that could be used to steal identities or cause financial fraud. At this time, it is not known which approach ExecuPharm will take, how many of their services are unavailable or whether they have a planned and tested incident response plan. Companies need to change their approach to ransomware rather than trying to recover after an incident, especially during these chaotic times with many employees working remotely, leaving more companies at risk."[9]

42. In fact, security company Proofpoint, which analyzed cyberattacks against Fortune 500 companies, found that phishing attacks more than doubled from 2017 to 2018 and pharmaceutical companies were the most targeted industry.[10] According to Proofpoint, "Recent targeted attacks on pharmaceutical and life sciences companies are telling. In our analysis of attacks against Fortune 500 companies, drug makers saw a 150% jump in impostor emails—one of the largest increases in any industry. In 2018, attackers targeted pharmaceutical companies an

[8] D. Riley, *Data stolen from outsourcing group ExecuPharm published after ransomware attack*, SILICONANGLE (Apr. 27, 2020), https://siliconangle.com/2020/04/27/data-stolen-outsourcing-group-execupharm-published-following-ransomware-attack/ (last visited Sept. 5, 2023).

[9] L. O'Donnell, *Hackers Leak Biopharmaceutical Firm's Data Stolen in Ransomware Attack*, THREATPOST (April 28, 2020), https://threatpost.com/hackers-leak-biopharmaceutical-firms-data-stolen-in-ransomware-attack/155237/ (last visited Sept. 5, 2023).

[10] C. Dimitriadis, *Stakes of security especially high in pharmaceutical industry*, CSO (Apr. 9, 2019), https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html (last visited Sept. 5, 2023).

average of 71 times per organization. Healthcare organizations as a whole received an average of 43 impostor emails in the first quarter of 2019."[11]

43. Pharmaceutical companies like Defendant are prime targets because of the information they collect and store, including valuable intellectual property, proprietary information about patented drugs, clinical trial information, data related to new technologies, and personal information of employees and patients—all extremely valuable on underground markets.

44. This was known and obvious to Defendant as it observed frequent public announcements of data breaches affecting pharmaceutical and other health-related industries and knew that information of the type they collected, maintained, and stored is highly coveted and a frequent target of hackers.

45. For example, in August 2014, after a cyber-attack on Community Health Systems, Inc., the Federal Bureau of Investigation (FBI) warned companies within the healthcare industry that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[12]

46. In early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a massive data breach exposing the names, addresses, Social Security numbers, dates of

[11] Solution Brief, *Clean Bill of Health: Securing Pharmaceutical and Life Science Firms with Proofpoint*, PROOFPOINT (Jan. 2020), https://www.proofpoint.com/sites/default/files/pfpt-us-sb-securing-pharmaceutical-and-life-science-firms.pdf (last visited Sept. 5, 2023).

[12] J. Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Sept. 5, 2023).

birth, and employment histories of nearly 80 million current and former plan members nationwide.[13]

47. In March 2015, health insurer Premera Blue Cross announced it suffered a data breach that exposed the medical data and financial information of 11 million customers, including claims data, clinical information, banking account numbers, Social Security numbers, birth dates and other data in a cyberattack that began in May 2014.[14]

48. In September 2015, New York-based heather insurer Excellus BlueCross BlueShield announced a breach that exposed the personal information of 10 million of its plan members in an attack dating back to 2013, including names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification numbers, financial account information and claim information.[15]

49. In June 2017, U.S.-based pharmaceutical giant Merck, an ExecuPharm client, was hit with a massive cyberattack that shut down the company's systems and sought a ransom in exchange for access.[16] Over the coming days, Merck's company-wide e-mail was disabled, 70,000 employees were prohibited from accessing their devices, and the organization suffered a

[13] C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (last visited Sept. 5, 2023).

[14] *Premera Blue Cross Says Data Breach Exposed Medical Data*, THE NEW YORK TIMES (March 1, 2015), https://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html (last visited Sept. 5, 2023).

[15] *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last visited Sept. 5, 2023).

[16] H. Shaban, *et al.*, *Pharmaceutical giant rocked by ransomware attack*, THE WASHINGTON POST (June 27, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/ (last visited Sept. 5, 2023).

worldwide disruption of its operations which forced a halt on the production of new drugs.[17] Due to a production shutdown caused by the attack, Merck experienced hundreds of millions of dollars in sales reductions and the attack reportedly cost Merck $1.3 billion in total losses.[18]

50. In April 2019, it was announced that German pharmaceutical giant Bayer was the target of an attempted cyberattack when the company discovered malware on its network in early 2018 and then isolated and monitored it over the coming months to track its source. Bayer's ability to contain the threat prevented a potential system-wide takeover that could have resulted in significant data loss and extensive operational disruption.[19]

51. In July 2019, Roche AG, a Swiss multinational healthcare and pharmaceutical company, acknowledged that it had been the target of a cyberattack that, like Bayer, involved a type of malware that allows hackers to remotely access the company's computer network.[20] Like Bayer, Roche was able to identify and contain the threat. According to a Roche spokesperson, "Roche has been targeted by various attackers in the past, including the group known as Winnti. These attacks were detected and remediated. Roche hasn't lost any sensitive personal data of our employees, patients, customers or business partners."[21]

---

[17] M. Erman, *et al*., *Merck says cyber attack halted production, will hurt profits*, REUTERS (July 28, 2017), https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO (last visited Sept. 5, 2023).

[18] D. Voreacos, *et al*., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG (Dec. 2, 2019), https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (last visited Sept. 5, 2023).

[19] P. Weiss, *et al*., *Bayer contains cyber attack it says bore Chinese hallmarks*, REUTERS (Apr. 4, 2019), https://www.reuters.com/article/us-bayer-cyber/bayer-says-has-detected-contained-cyber-attack-idUSKCN1RG0NN (last visited Sept. 5, 2023).

[20] A. Schuetze, *et al*., *BASF, Siemens, Henkel, Roche target of cyber attacks*, REUTERS (July 24, 2019), https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147 (last visited Sept. 5, 2023).

[21] E. Palmer, *Roche, like Bayer, was hit in Winnti cyberattack*, FIERCE PHARMA (July 24, 2019), https://www.fiercepharma.com/manufacturing/roche-like-bayer-was-targeted-winnti-cyber-attack (last visited Sept. 5, 2023).

52. In addition to these cyberattacks targeting the healthcare and pharmaceutical industries, among hundreds of others, Defendant also observed numerous other well-publicized data breaches involving major corporations that were targeted given the sensitive consumer information they retained. For example, through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when users' names, addresses, and dates of birth were stolen as part of a multi-faceted cyberattack.[22]

53. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.[23]

54. In September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of 147 million Americans between May and July 2017.[24] The following year, hotel giant Marriott announced that 383 million guest records were exfiltrated from its hotel guest reservation database over a four-year period.[25]

55. Despite being a holder of highly sensitive information, ExecuPharm failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access on its network. Defendant had the resources to prevent a breach and made

[22] S. Larson, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (OCT. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (last visited Sept. 5, 2023).

[23] B. Krebs, *Home Depot Hit By Same Malware as Target*, KREBS ON SECURITY (Sept. 14, 2014), https://krebsonsecurity.com/tag/home-depot-databreach/ (last visited Sept. 5, 2023).

[24] Equifax Press Release, *Equifax 2017 Cybersecurity Incident & Important Consumer Information*, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 5, 2023).

[25] Marriott Press Release, *Marriott Provides Update on Starwood Database Security Incident*, https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/ (last visited Sept. 5, 2023).

significant expenditures to promote their business operations, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting pharmaceutical, healthcare, and other related industries.

Allegations Relating to Plaintiff

56. Plaintiff was hired by ExecuPharm in February 2016 as a clinical technical editor where she was responsible for quality control of regulatory documents.

57. As a condition of her employment, Plaintiff provided ExecuPharm with significant amounts of her personal and financial information, including her name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information, as well as her passport or other forms of identification. Plaintiff also provided ExecuPharm with Personal Information relating to her husband and minor daughter.

58. As a further condition of her employment, Plaintiff was required to execute an employment agreement with ExecuPharm in which the company promised and agreed to take "appropriate measures" to protect her personal information:

> **Personal Data**. Employee consents to the lawful collection, storing and processing of personal data of Employee. Such personal data may be processed and stored in internal databases that may be accessible from other areas and other countries. The personal data may be used to administer and manage matters relating to this Agreement and in order to comply with any potential applicable regulatory requirements. The Company may transfer such personal data, consistent with applicable law, to any of its affiliates, representatives, contractors or other individuals it deems appropriate. **Company will take appropriate measures to protect the confidentiality and security of all personal data**.

59. Plaintiff ended her employment with ExecuPharm in November 2016 to pursue another opportunity. Because ExecuPharm continued to retain Plaintiff's Personal Information, ExecuPharm's contractual obligation "to protect the confidentiality and security of [her] personal data" extended beyond the termination of her employment.

60. On March 20, 2020, Plaintiff received an e-mail from ExecuPharm notifying her of the Data Breach and informing her that her "sensitive information has been accessed, including [her] social security number, banking information (copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including social security numbers) and payroll tax forms (such as W-2 and W-4). For some employees, copies of passports also were accessed." Attached to the e-mail was a PDF of the initial notification letter dated March 18, 2020, which Plaintiff did not previously receive.

61. Given the significant amount of highly-sensitive information compromised, Plaintiff became fearful for the safety, security, and financial well-being of herself and her family. As a result, she followed the guidance in ExecuPharm's communication and began reviewing her financial records and credit reports for unauthorized activity and contacting her financial institutions and credit bureaus to inquire about placing fraud alerts.

62. On March 23, 2020, Plaintiff attempted to call ExecuPharm's "dedicated hotline" to inquire about the credit monitoring services being offered and seek additional information beyond what was made available in the notice letters. Despite making multiple calls, Plaintiff was unable to reach anyone as the phone number was non-operational.

63. On March 24, 2020, Plaintiff called the dedicated hotline again and this time was able to speak to a call center operator. The operator provided scripted responses to Plaintiff's

questions and was unable to give any additional information beyond what was already provided in ExecuPharm's earlier communications.

64. On April 26, 2020, Plaintiff received an e-mail from ExecuPharm confirming that her family's most sensitive personal and financial was "shared on the dark web." At no point prior to this communication did ExecuPharm disclose that the hackers behind the cyberattack were a known ransomware group that threatened to release the information if their demands were not met more than six weeks prior. Neither did ExecuPharm disclose what specific information was compromised relating to each affected individual, as it represented it would do.

65. In response to this new information, Plaintiff sent a message to a dedicated e-mail address created for employee inquiries regarding the Data Breach that stated: "Given this even more disturbing turn of events and knowledge that our personal information has been shared on the dark web, is [ExecuPharm] going to do anything additional to support those of us impacted? One year of credit monitoring is likely not enough given these circumstances and that identity thieves often wait more than 1 year to do harm."

66. Three days later, an ExecuPharm representative responded: "Thank you for your email. ExecuPharm's decision to offer free identity monitoring for one year to all employees and alumni who may have been impacted by the data security incident is a reasonable timeframe and consistent with best practices. If you have any more questions, please let us know."

67. As a result of the Data Breach, Plaintiff has suffered a variety of injuries and harm. She has spent significant time and effort reviewing her financial accounts, bank records, and credit reports for unauthorized activity and will continue to do so. After placing a security alert on her financial account, Plaintiff was unable to deposit a check she received from work as the transaction was flagged and she was delayed from accessing her own money.

68. Thereafter, Plaintiff and her husband transferred their joint account to a new bank, which was a time-consuming process, and undertook the process of changing their bank account numbers for their entire family. This required Plaintiff, her husband, and minor daughter to drive to their financial institution in the middle of the COVID-19 pandemic and spend more than an hour meeting with bank personnel and filling out forms, all while putting the health of Plaintiff and her family at risk.

69. Thereafter, Plaintiff had to update all the accounts tied to her previous account numbers, including her payroll direct deposit. Due to a mistake by the bank, the new account number was inaccurately transcribed, which was discovered only after Plaintiff did not receive a scheduled electronic payment. Again, Plaintiff was delayed from accessing her funds and had to spend hours sorting through the issue with her payroll department and bank.

70. Because these issued had to be addressed during normal business hours, Plaintiff was forced to miss time from work taking mitigative measures. This caused Plaintiff to work late nights to make up for the hours spent addressing issues resulting from the Data Breach.

71. Plaintiff also placed fraud alerts and later credit freezes on her credit reports with the major credit bureaus and enrolled in the one year of credit monitoring services offered by ExecuPharm. Knowing such services would expire after only a year and would not cover her family, Plaintiff later purchased three-bureau credit monitoring services for herself and her family at a cost of $39.99 per month so that they can monitor their credit profiles for fraudulent activity.

72. In addition to spending time, money, and effort as a result of the Data Breach, Plaintiff has suffered stress and anxiety worrying about the safety and financial well-being of herself and her family. Plaintiff sought and paid for counseling services to help cope in part with the stress caused by the Data Breach.

73. In March 2023, Plaintiff received an alert from her credit card company that her Social Security number had been located on the dark web. Given the highly sensitive nature of the information stolen, the value of Plaintiff's Personal Information has been diminished and she remains at a substantial and imminent risk of future harm.

Defendant Failed to Comply with Regulatory Guidance

74. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[26]

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[27] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

[26] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Sept. 5, 2023).

[27] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 5, 2023).

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28]

76. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[30]

78. In this case, Defendant was fully aware of its obligation to use reasonable measures to protect the personal information of its customers, with ExecuPharm promising as much in its own employment agreement. Defendant also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, ExecuPharm failed to protect its highly-sensitive data.

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[28] *Id.*

[29] FTC, *Start With Security*, *supra* note 26.

[30] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Sept. 5, 2023).

The Effect of the Data Breach on Affected Individuals

80. Given the highly sensitive nature of the Personal Information stolen in the Data Breach, and its subsequent publication on underground websites, fraudsters across the globe have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and class members now and indefinitely into the future.

81. In fact, many victims of the Data Breach have already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, medical and healthcare fraud, unauthorized financial accounts or lines of credit opened in their names, and fraudulent payment card purchases. Plaintiff and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, replacing passports, checking credit reports, and spending time and effort searching for unauthorized activity.

82. The Personal Information exposed in the Data Breach—including full names, home addresses, social security numbers, taxpayer IDs, credit card numbers, banking information (including copies of personal checks for direct deposit), driver's licenses, dates of birth, names of spouses and beneficiary information, including their social security numbers, payroll tax forms (such as W-2 and W-4 forms), and copies of passports—is highly-coveted and valuable on underground markets. Identity thieves can use the Personal Information to (i) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (ii) reproduce stolen debit cards and use them to withdraw cash from ATMs; (iii) commit immigration fraud; (iv) obtain a fraudulent driver's license or ID card in the victim's name; (v) obtain fraudulent government benefits or medical treatment; (vi) file a fraudulent tax return using the victim's information; (vii) commit passport fraud; (viii) commit medical or healthcare-related fraud; (ix)

commit espionage; or (x) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

83. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[31] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

84. Victims who had their passports compromised are at an even greater risk of harm. Hackers can combine exposed passport numbers with other personal information to create false identities or fraudulent passports, which are "often linked to illegal immigration, contraband smuggling, economic crimes, international terrorism and other serious crimes."[32] According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding passport fraud:

> Fraudulent passports pose a significant risk because they can be used to conceal the true identity of the user. In addition, according to the Department of State (State), passport and visa fraud are often committed in connection with crimes such as international terrorism, drug trafficking, organized crime, alien smuggling, money laundering, pedophilia, and murder. As a result, even a few instances of passport fraud can have far-reaching effects.[33]

---

[31] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Sept. 5, 2023).

[32] *Passport Fraud - Protect Your Passport and Avoid Identity Theft*, U.S. PASSPORT SECURITY GUIDE, https://www.us-passport-service-guide.com/passport-fraud.html (last visited Sept. 5, 2023).

[33] U.S. Government Accountability Office Report to Congressional Requesters, *Pervasive Passport Fraud Not Identified, but Cases of Potentially Fraudulent and High-Risk Issuances Are under Review* (May 2014), https://www.gao.gov/assets/670/662921.pdf (last visited Sept. 5, 2023).

85. For this reason, passport information is a valuable commodity on underground markets, especially when it is paired with other data points tied to an individual such as those exposed in the Data Breach. For victims who opt to replace their passports, the multi-step process is time consuming and costly. They must first report the loss to the U.S. State Department so that the passport will be invalidated and cannot be used for travel. This requires filling out a Form DS-64, which requires an explanation of how the passport was lost or stolen and the submission of the identifying information of the passport-holder including full name, address, place of birth, and Social Security number, among other personal information.

86. Next, the victim must get new passport photos taken, which typically cost $15 or more at the U.S. Post Office. The applicant then has to travel in-person to a passport acceptance facility to apply for a new passport. This requires providing a copy of a U.S. birth certificate or certificate of naturalization or citizenship, a government-issued photo ID, and the new passport photos. The cost of obtaining a new passport is $140 for a passport book and card, plus an additional $35 acceptance fee to obtain the passport through an authorized passport acceptance facility. The applicant must then wait weeks or even months for the new passport to arrive.

87. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety

- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.[34]

88. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[35]

89. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[36]

---

[34] *Identity Theft Resource Center*, *supra* note 31.

[35] *Id.*

[36] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Sept. 5, 2023).

90. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[37]

91. The unauthorized disclosure of the sensitive Personal Information to data thieves also reduces its inherent value to its owner. As one court recently recognized: "Consumers recognize the value of their personal information and offer it in exchange for goods and services. To take a few examples, many business[es] offer goods and services such as wifi access, special access to products, or discounts in exchange for a customer's personal information. Consumer[s] choose whether to exchange their personal information for these goods and services every day. . . . [T]he value of personal identifying information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal identifying information. .

[37] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 5, 2023).

. . Similarly, the businesses that request (or require) consumers to share their personal identifying information as part of a commercial transaction do so with the expectation that its integrity as not been compromised." *In re Marriott International, Inc., Customer Data Sec. Breach Litig.*, --- F. Supp. 3d ---, 2020 WL 869241, at *8 (D. Md. Feb. 21, 2020).

92. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

93. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their Personal Information;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, cancelling and reissuing cards, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

94. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[38]

95. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[39]

96. Although ExecuPharm told Plaintiff and class members that it is "critical" they activate the credit monitoring services "to help mitigate your risk of identity theft"—in reality

[38] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 5, 2023).

[39] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Sept. 5, 2023).

credit monitoring is reactionary, it cannot mitigate the "risk of identity theft" because it is not a preventative tool. Instead, credit monitoring can alert someone to identity theft or fraud *after it has already occurred* so that hopefully the harm can be mitigated. Additionally, and contrary to ExecuPharm's representations, one year of credit monitoring is woefully inadequate as Plaintiff and class members will need to monitor their credit profiles for identity theft and fraud indefinitely given the nature of the information stolen. Consequently, ExecuPharm's representation to Plaintiff that one year of monitoring is a "reasonable timeframe and consistent with best practices" is flatly incorrect.

97. As a result of Defendant's failure to protect the Personal Information they were entrusted to safeguard, Plaintiff and class members have been placed at an imminent and ongoing risk of harm from identity theft and identity fraud, requiring them to spend time, money, and effort to mitigate the actual and potential impact of the Data Breach on their lives including, but limited to, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their financial accounts and credit reports for unauthorized activity.

98. ExecuPharm expressly acknowledged the imminent risk of harm affected individuals now face. It warned those affected that "[u]nauthorized access to such information may potentially lead to the misuse of your personal data to impersonate you and/or to commit, or allow third parties to commit, fraudulent acts such as securing credit in your name" and advised Plaintiff and class members to "act diligently and immediately in the face of heightened likelihood of bad actors using your information unlawfully and/or without your consent" and to "take every precautionary measure" including to:

- Place a fraud alert on your credit file (creditors will contact you before they open new accounts or change your existing accounts)

- Check your credit report (and freeze your credit if you have concerns)
- Change passwords to any personal and professional accounts that may have been accessed on the ExecuPharm server
- Speak with your bank representative for specific guidance on any changes that may be needed to your bank account(s).
- Actively monitor financial statements for suspicious activity; and
- File taxes as soon as possible to mitigate any potential fraudulent tax filing activity.

99. Further, Defendant continues to hold Plaintiff and class members' Personal Information, and, therefore, they have an interest in ensuring that their Personal Information is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

100. Plaintiff seeks relief individually and as a representative of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

> All persons whose Personal Information was compromised as a result of the data breach announced by ExecuPharm on or about March 20, 2020 (the "Class").

101. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiff also seeks certification of the following subclass defined as follows:

> All persons whose Personal Information was compromised as a result of the data breach announced by ExecuPharm on or about March 20, 2020 and who entered into an employment agreement with ExecuPharm in which ExecuPharm promised and agreed to take appropriate measures to protect the confidentiality and security of the employee's personal data (the "ExecuPharm Employee Subclass").

102. Excluded from the Class and Subclass is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded

from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

103. Plaintiff reserves the right to propose other subclasses and amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

104. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiff at this time, preliminary information suggests there are thousands of individuals whose Personal Information was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. mail, internet postings, and/or published notice.

105. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include, but are not limited to:

a. Whether Defendant knew or should have known of the susceptibility of ExecuPharm's systems to a data breach;

b. Whether ExecuPharm failed to implement reasonable and adequate security procedures and practices;

c. Whether ExecuPharm's security measures to protect its systems were reasonable in light of known legal requirements;

d. Whether Defendant took adequate measures to protect Plaintiff and class members' Personal Information after evidence of unauthorized access on ExecuPharm's network was discovered;

e. Whether Defendant owed a duty to Plaintiff and class members to protect their Personal Information;

f. Whether Defendant breached its duty to protect the Personal Information of Plaintiff and class members by failing to provide adequate data security;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of ExecuPharm's systems and/or the loss of the Personal Information of Plaintiff and class members;

h. Whether Defendant had a contractual obligation to use reasonable security measures and whether they complied with such contractual obligations;

i. Whether, as a result of Defendant's conduct, Plaintiff and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and,

j. Whether, as a result of Defendant's conduct, Plaintiff and class members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

106. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other class members. Like other class members, Plaintiff's Personal Information was in ExecuPharm's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other class members and Plaintiff seeks relief consistent with the relief of the Class.

107. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate class representative because her interests do not conflict with the interests of class members who she seeks to represent. Plaintiff has retained counsel that is competent and experienced in complex class action litigation and data breach and privacy litigation. Plaintiff and her counsel intend to vigorously prosecute this action and the interests of class members will be fairly and adequately protected by Plaintiff and her counsel.

108. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

109. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

110. Likewise, particular issues are appropriate for certification under Rule 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant failed to take reasonable steps to safeguard the Personal Information of Plaintiff and class members;

c. Whether Defendant failed to adequately monitor and audit the data security systems of ExecuPharm.

CHOICE OF LAW ALLEGATIONS

111. Pennsylvania law applies to the claims of all class members.

112. ExecuPharm's employment agreement with Plaintiff states that: "This Agreement shall be governed by the laws of the Commonwealth of Pennsylvania, and any action brought under or pertaining to this Agreement or Employee's employment shall be brought exclusively in the Pennsylvania Court of Common Pleas for Montgomery County or the United States District Court for the Eastern District of Pennsylvania. The Company and Employee submit to the exclusive jurisdiction of such courts."

113. Further, the Commonwealth of Pennsylvania has sufficient contacts to Defendant's conduct for Pennsylvania law to be uniformly applied to the claims of Plaintiff and the Class. Application of Pennsylvania law to all class members' claims comports with the Due Process Clause given the significant aggregation of contacts between Defendant's conduct and this Commonwealth.

114. The conduct that forms the basis for the claims of Plaintiff and the Class against Defendant is the theft of their Personal Information from ExecuPharm, which is headquartered and does substantial business in Pennsylvania.

115. Pennsylvania has a greater interest than any other state in applying its law to the claims at issue in this case. Pennsylvania has a very strong interest in ensuring that its resident corporations implement and maintain reasonable data security practices and protect the sensitive personal information they collect, as well as ensuring that harm inflicted on affected individuals is redressed. Pennsylvania's interest in preventing unlawful corporate behavior occurring in Pennsylvania substantially outweighs the interest of any other state. If other states' laws were applied to class members' claims, Pennsylvania's interest in deterring resident corporations from failing to implement and maintain reasonable data security practices would be impaired.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class against Defendant)

116. Plaintiff restates and re-alleges paragraphs 1 through 115 of this Complaint, as if fully set forth herein.

117. Defendant owed a duty to Plaintiff and members of the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting the Personal Information they collected from ExecuPharm's employees as a condition of their employment from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing ExecuPharm's security systems to ensure that the Personal Information in ExecuPharm's possession was adequately secured and protected.

118. Defendant owed a duty of care to Plaintiff and members of the Class to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected the Personal Information of their current and former employees.

119. Defendant had a special relationship with Plaintiff and class members. Plaintiff and class members' willingness to entrust Defendant with their Personal Information as a condition of employment was predicated on the understanding that Defendant would take adequate security precautions to protect their Personal Information.

120. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of inadequate security practices. Defendant knew or should have known they were targets of cyberattacks and the critical importance of adequately securing their employees' Personal Information.

121. Plaintiff and members of the Class entrusted Defendant with their Personal Information with the understanding that Defendant would safeguard their information, as well as the information of their dependents and beneficiaries.

122. Defendant's conduct also created a foreseeable risk of harm to Plaintiff and members of the Class by failing to: (1) secure ExecuPharm's systems and exercise adequate oversight of ExecuPharm's data security protocols; (2) ensure compliance with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

123. ExecuPharm knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of ExecuPharm's systems, and the importance of adequate security. ExecuPharm was aware of numerous, well-publicized data breaches within the pharmaceutical and healthcare industries in the months and years preceding the Data Breach.

124. ExecuPharm's duties to use reasonable care in protecting Personal Information also arise from common law and statutes and regulations such as the FTC Act, as well as its own promises regarding privacy and data security.

125. ExecuPharm breached its common law duty to act with reasonable care in collecting and storing the Personal Information of their employees, which exists independently from any contractual obligations between the parties. Specifically, ExecuPharm breached its common law, statutory, and other duties to Plaintiff and class members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiff and class members' Personal Information;

c. storing former employees' Personal Information longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

126. ExecuPharm's failure to implement implemented and maintained adequate data security measures to protect the Personal Information of Plaintiff and class members created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiff and members of the Class did not contribute to the Data Breach or the subsequent misuse of their Personal Information as described herein.

127. As a direct and proximate result of ExecuPharm's conduct, Plaintiff and the Class have and will suffer damages including, but not limited to: (i) the loss of value of their Personal Information and loss of opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as ExecuPharm fails to undertake appropriate and adequate measures to protect it; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class against Defendant)

128. Plaintiff restates and re-alleges paragraphs 1 through 115 of this Complaint, and asserts this claim in the alternative to her breach of contract claim against ExecuPharm to the extent necessary.

129. As a condition of their employment, Plaintiff and members of the Class were required to provide their Personal Information to Defendant.

130. Implicit in the agreement between Defendant and its employees was the obligation that Defendant would implement and maintain reasonable safeguards to protect employees' information and comply with industry-standard data security practices.

131. Additionally, Defendant implicitly promised and agreed to retain this Personal Information only under conditions that kept such information secure and confidential and only as

long as reasonably necessary to perform essential business functions. As such, Defendant had a duty to reasonably safeguard and protect the Personal Information of Plaintiff and Class members from unauthorized disclosure or access.

132. Defendant breached their implied agreement with Plaintiff and members of the Class by failing take appropriate measures to protect the confidentiality and security of their personal data, resulting in the Data Breach.

133. As a direct and proximate result of Defendant's breach, Plaintiff and members of the Class suffered injury and sustained actual losses and damages as described herein.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and the ExecuPharm Employee Subclass against ExecuPharm)

134. Plaintiff restates and re-alleges paragraphs 1 through 115 of this Complaint, as if fully set forth herein.

135. As a condition of their employment, Plaintiff and members of the ExecuPharm Employee Subclass were required to provide their Personal Information to ExecuPharm.

136. As a further condition of their employment, Plaintiff and members of the ExecuPharm Employee Subclass were required to execute an employment agreement with ExecuPharm in which the company promised and agreed to "take appropriate measures to protect the confidentiality and security of all [employee's] personal data."

137. ExecuPharm breached its agreement with Plaintiff and members of the ExecuPharm Employee Subclass by failing take appropriate measures to protect the confidentiality and security of their personal data, resulting in the Data Breach.

138. As a direct and proximate result of ExecuPharm's breach, Plaintiff and members of the ExecuPharm Employee Subclass suffered injury and sustained actual losses and damages as described herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the ExecuPharm Employee Subclass against ExecuPharm)

140. Plaintiff restates and re-alleges paragraphs 1 through 115 of this Complaint, as if fully set forth herein.

141. ExecuPharm had a fiduciary relationship with Plaintiff and similarly situated members of the ExecuPharm Employee Subclass, in that:

a. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass, during the course of their employment with ExecuPharm, relied upon compensation they received through said employment to support themselves and their families;

b. ExecuPharm is a subsidiary and functional service arm of Parexel International Corp., a global biopharmaceutical corporation with annual sales of more than $2.4 billion and employing more than 18,000 people;

c. The employment of Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass was "at-will", meaning their employment and means of basic financial support could be terminated at any time and for any reason, or for no reason at all;

d. ExecuPharm thus did not deal with Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass on equal terms, but instead from a position of overmastering dominance, and by contrast,

Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass dealt from a position of weakness and dependence in their relationship with ExecuPharm;

e. As a result of this imbalance, ExecuPharm was able to extract from Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass significant amounts of their highly sensitive personal information as a condition of employment. ExecuPharm required Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass to provide it, for instance, their addresses, Social Security numbers, bank and financial account information, insurance information, tax information, passports, and other forms of identification, along with similar information relating to their family members and dependents;

f. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass provided much of this sensitive personal information to ExecuPharm after they had formed a fiduciary relationship with ExecuPharm, and after they had become justifiably reliant on ExecuPharm for ongoing employment and compensation;

g. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass were required to provide the sensitive personal information in question as a condition of employment, such that their employment would be terminated if they had declined to provide it to ExecuPharm;

h. ExecuPharm expressly and affirmatively promised to "take appropriate measures to protect the confidentiality and security of all personal data" provided by Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass;

i. In justifiable reliance upon this promise, Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass surrendered control of their sensitive personal information to ExecuPharm such that they had no input whatsoever concerning how it was used, and ExecuPharm maintained the unfettered right to use it in any manner it chose without any subsequent authorization or consent from Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass; and

j. The sensitive personal information in question constituted a substantial portion of the affairs of Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass in that it included information concerning and relating to their identities, financial conditions, home addresses, and familial relationships, as well as substantial information useful to malicious actors able to misuse it for financial gain.

142. By failing to implement and maintain reasonable safeguards to protect their employees' Personal Information, failing to comply with industry-standard data security practices, failing to disclose critical information regarding the nature of the Data Breach, and allowing a third-party hacker to release their Personal Information on the dark web, ExecuPharm intentionally or negligently failed to act in good faith and solely for the benefit of Plaintiff and members of the ExecuPharm Employee Subclass.

143. ExecuPharm's failure to act solely for the benefit of Plaintiff and members of the ExecuPharm Employee Subclass was a real and meaningful factor in bringing about their injuries.

144. As a direct and proximate result of ExecuPharm's breach of fiduciary duty, Plaintiff and members of the ExecuPharm Employee Subclass suffered injury and sustained actual losses and damages as described herein.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the ExecuPharm Employee Subclass against ExecuPharm)

145. Plaintiff restates and re-alleges paragraphs 1 through 115 of this Complaint, as if fully set forth herein.

146. As a condition of their employment, Plaintiff and members of the ExecuPharm Employee Subclass were required to provide their Personal Information to ExecuPharm. Such information was highly personal, sensitive, and not generally known.

147. ExecuPharm expressly and implicitly agreed to protect the confidentiality and security of the Personal Information it collected, stored, and maintained.

148. ExecuPharm had a confidential relationship with Plaintiff and similarly situated members of the ExecuPharm Employee Subclass, in that:

a. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass, during the course of their employment with ExecuPharm, relied upon compensation they received through said employment to support themselves and their families;

b. ExecuPharm is a subsidiary and functional service arm of Parexel International Corp., a global biopharmaceutical corporation with annual sales of more than $2.4 billion and employing more than 18,000 people;

c. The employment of Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass was "at-will", meaning their employment and means of basic financial support could be terminated at any time and for any reason, or for no reason at all;

d. ExecuPharm thus did not deal with Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass on equal terms, but instead from a position of overmastering dominance, and by contrast, Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass dealt from a position of weakness and dependence in their relationship with ExecuPharm;

e. As a result of this imbalance, ExecuPharm was able to extract from Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass significant amounts of their highly sensitive personal information as a condition of employment. ExecuPharm required Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass to provide it, for instance, their addresses, Social Security numbers, bank and financial account information, insurance information, tax information, passports, and other forms of identification, along with similar information relating to their family members and dependents;

f. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass provided much of this sensitive personal information to ExecuPharm after they had formed a confidential relationship with

ExecuPharm, and after they had become justifiably reliant on ExecuPharm for ongoing employment and compensation;

g. Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass were required to provide the sensitive personal information in question as a condition of employment, such that their employment would be terminated if they had declined to provide it to ExecuPharm;

h. ExecuPharm expressly and affirmatively promised to "take appropriate measures to protect the confidentiality and security of all personal data" provided by Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass;

i. In justifiable reliance upon this promise, Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass surrendered control of their sensitive personal information to ExecuPharm such that they had no input whatsoever concerning how it was used, and ExecuPharm maintained the unfettered right to use it in any manner it chose without any subsequent authorization or consent from Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass; and

j. The sensitive personal information in question constituted a substantial portion of the affairs of Plaintiff and other similarly situated members of the ExecuPharm Employee Subclass in that it included information concerning and relating to their identities, financial conditions, home addresses, and

familial relationships, as well as substantial information useful to malicious actors able to misuse it for financial gain.

149. ExecuPharm disclosed the Personal Information to unauthorized third parties by failing to implement and maintain reasonable safeguards to protect its employees' Personal Information and failing to comply with industry-standard data security practices.

150. As a direct and proximate result of ExecuPharm's breach of confidence, Plaintiff and members of the ExecuPharm Employee Subclass suffered injury and sustained actual losses and damages as described herein.

COUNT VI
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class against Defendant)

151. Plaintiff restates and re-alleges paragraphs 1 through 116 of this Complaint, as if fully set forth herein.

139. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state and federal statutes described in this Complaint.

140. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and class members from further cyberattacks and data breaches that compromise their Personal Information.

141. Defendant still possesses Personal Information pertaining to Plaintiff and class members, which means their Personal Information remains at risk of further breaches because

Defendant's data security measures remain inadequate. Plaintiff continues to suffer injuries as a result of the compromise of her Personal Information and remains at an imminent risk that further compromises of their Personal Information will occur in the future.

142. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendant's existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, ExecuPharm must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' Personal Information if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on ExecuPharm's systems on a periodic basis, and ordering ExecuPharm to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. encrypting Personal Information and segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of ExecuPharm's systems is compromised, hackers cannot gain access to other portions of ExecuPharm's systems;

e. purging, deleting, and destroying in a reasonable and secure manner Personal Information not necessary to perform essential business functions;

f. conducting regular database scanning and security checks;

g. conducting regular employee education regarding best security practices;

h. implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all class members, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

A. For an Order certifying the Class and subclass, as defined herein, and appointing Plaintiff as the class representative and the undersigned counsel as class counsel;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and class member's Personal Information;

C. For equitable relief compelling Defendant to use industry-standard security methods and policies with respect to data collection, storage and protection, and sharing of information, and to dispose of Plaintiff's and class members' Personal information in their possession that is not necessary to perform essential business functions;

D. For an award of damages, including nominal and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowable by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Date: September 6, 2023

Respectfully submitted,

/s/ *Mark S. Goldman*
Mark S. Goldman (PA Bar No. 48049)
GOLDMAN SCARLATO & PENNY, P.C.
161 Washington Street, Suite 1025
Conshohocken, Pennsylvania 19428
Telephone: (484) 342-0700
goldman@lawgsp.com

Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Caleb J. Wagner (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
wagner@stuevesiegel.com

Attorneys for Plaintiff and the Proposed Classes

CERTIFICATE OF SERVICE

I hereby certify that on September 6, 2023, a true and correct copy of the foregoing document was filed electronically through the Court's CM/ECF system, and therefore, will be transmitted to all counsel of record by operation of the Court's CM/ECF system.

/s/ *Mark S. Goldman*
Attorney for Plaintiff